DSCP-DOD-Medical Device Vendor Industrial Conference

Defense Information Technology Security Certification & Accreditation Process (DITSCAP)

Air Force Medical Support Agency (AFMSA)
Clinical Engineering Branch
Fort Detrick Maryland

27 Sept 04

Goals

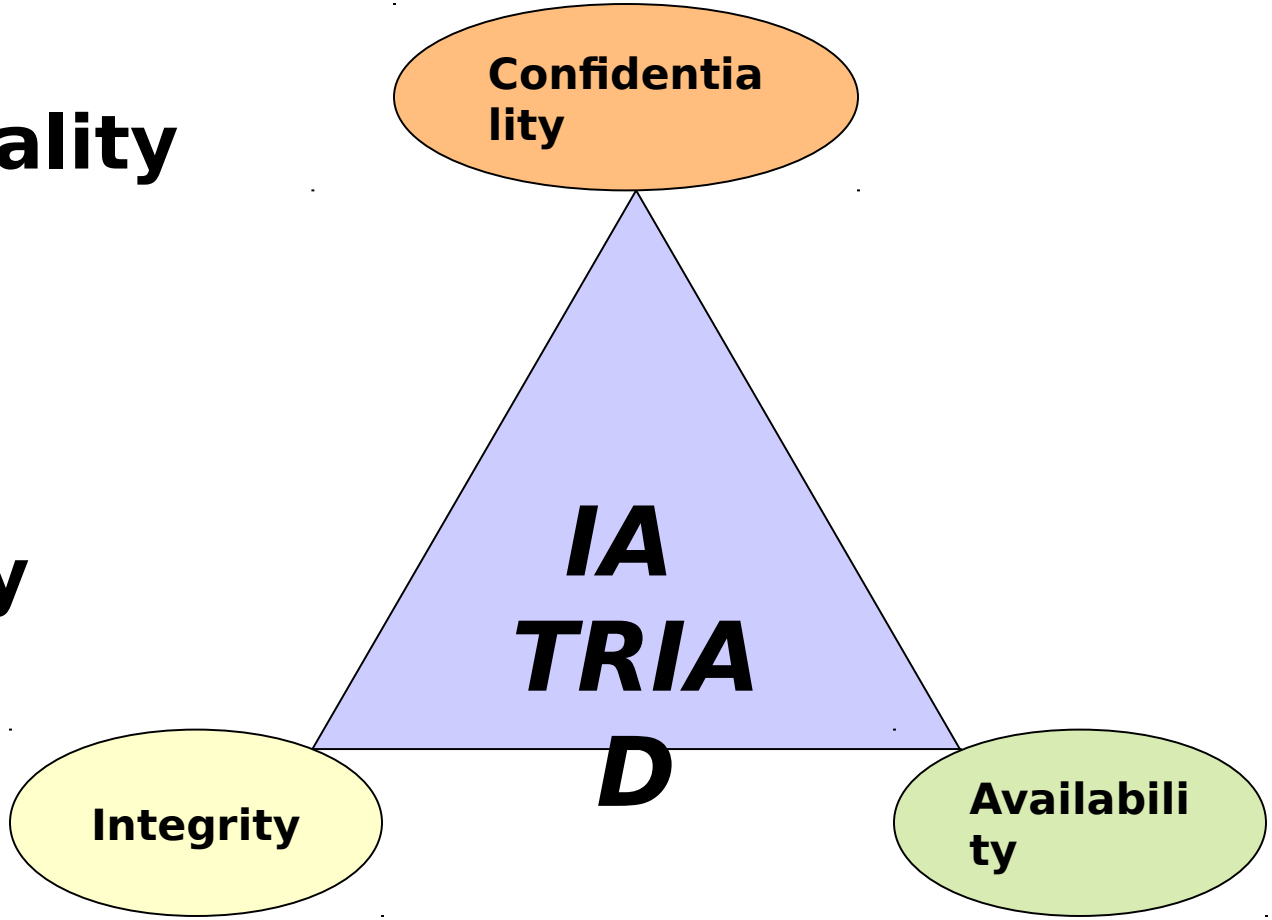
- **Clarity**
  - ✓ Background – Why DITSCAP?
  - ✓ What DITSCAP is
  - ✘ What DITSCAP is NOT
- **Collaboration**
  - ✓ Feedback
  - ✓ Existing Processes
  - ✓ Commercial Sector Impact

Background – Why DITSCAP?

- **The "shift" to the Network**
  - ✓Internet
  - ✓Computerized Patient Record (CPR)
  - ✓HIPAA
- **The Increased Threat**
  - ✓Global Environment – Global Threat
  - ✓Software Vulnerabilities
- **Information Assurance (IA)**
  - ✓Certification
  - ✓Accreditation

Goals – “Keep the CIA in Mind”

- **Confidentiality**
- **Integrity**
- **Availability**



DITSCAP – What it is

- **Certification of the "System"**
  - ✓Validation - Functional Security Requirements
  - ✓Provides Assurance of IA Controls
    - Risk Analysis of System
    - Security Test & Evaluation (ST&E)
    - System Vulnerability Scans (e.g. ISS)
    - Security Technical Implementation Guides (STIGs)
  - ✓Results are Documented for Management
    - Residual Risks
    - Certifier Provides "Certification" Statement
    - Recommendation to Management

DITSCAP – What it is

- **Accreditation of the "System"**
  - ✓Senior Management's Formal Acceptance
    - Designated Approval Authority (DAA)
  - ✓Based on Certification Feedback
    - Residual Risk Assessment
    - Network Vulnerability Assessment
    - Certification Statement
  - ✓Formal Risk Acceptance
    - Based on Documented Residual Risks
    - Based on Documented Mitigation Measures
    - Based on Documented System Architecture

DITSCAP – What it is NOT

- **Static (i.e. One-Time)**
  - ✘ Dynamic Process Over the System Life Cycle
  - ✘ Reaccreditation Every Three Years
  - ✘ When a *Major* Change is Implemented
- **"AFCA Testing"**
  - ✘ Enterprise Network Assessment
    - Bandwidth
    - Interoperability
    - Password Security
  - ✘ Certificate of Networthiness – i.e. CON

DITSCAP – Collaboration

- **Requires Vendor Input**
  - ✓System Manuals – Security Tools
  - ✓System Ports and Protocols
  - ✓System Architecture
- **Existing Products, Processes, and Support**
  - ✓Systems Administrators Manuals
  - ✓FDA/510(k) and GMP
- **A Collaborative Effort to Achieve "CIA"**
  - ✓DOD May be First – the Commercial Market is

DITSCAP

- **Clarity**
  - ✓ Background – Why DITSCAP?
  - ✓ What DITSCAP is
  - ✘ What DITSCAP is not
- **Collaboration**
  - ✓ Feedback
  - ✓ Existing Processes
  - ✓ Commercial Sector Impact
- **Questions?**

Defense Information Technology Security Certification and Accreditation (DITSCAP)

Mr. Mike Durnen
DISA/IN
(703) 681-2626

UNCLASSIFIED

DITSCAP OVERVIEW

WHAT IS DITSCAP?

DoD Information Technology Security Certification and Accreditation Process – It establishes a standard DOD-wide process, set of activities, general tasks, and a management structure to certify and accredit Information Systems (IS) that will maintain the Information Assurance (IA) and security posture of the Defense Information Infrastructure (DII) throughout the life cycle of the system.

- DoD Instruction 5200.40 (DITSCAP), ASD Signature 30 Dec 97
- DoD 8510.1-M (DITSCAP Application Manual), ASD Signature 31 Jul 00

WHY DITSCAP?

- It defines a process for uniform C&A practice
- It is applicable throughout the life cycle of system
- It is applicable to any type of acquisition strategy or development
- It should be part of the Acquisition Strategy
- It is a continuous process
- It brings responsible organizations together

APPLICABILITY?

Applies to

- All DOD CINCs/Services/Agencies, Components, Activities, CJCS, and their Contractors and Agents (DODI 5200.40, Para 2)
- “the acquisition, operation and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information”
- “Any IT or information system life cycle, …, the reconfiguration or upgrade of existing systems…”

Effective immediately

Mandatory for use by all DOD

FOUR PHASES of DITSCAP

PHASE 1

PHASE 2

PHASE 3

PHASE 3

- Review configuration & security Mgmt*
  - Follow change mgmt documented in SSAA
  - Determine if system security mgmt continues to support mission and architecture
- Conduct risk management review
  - Assess if risk to CIAA is being maintained at an acceptable level
- Conduct compliance validation if needed
  - Ensure continued compliance w/SSAA reqs, current threat assessment, and concept of operations
- Maintain SSAA

KEYS to DITSCAP PROCESS

Preparation and submission of a SSAA

- Adequately describes the system and its components
- Adequately addresses security requirements and security measures in place
- Includes diagrams that adequately reflect the system's architecture and location

Security Test and Evaluation (ST&E)

- Assess implementation of security design
- Ascertain that CIAA are implemented as documented in SSAA and perform properly
- Validate correct implementation of Identification & Authentication, Audits, Access Controls, Object Reuse, Trusted Recovery, and Network Connection Rule Compliance
- Evaluate system conformance w/reqs, mission, and architecture as defined in SSAA